The law and economics of cyber risk pooling

NEW YORK UNIVERSITY
JOURNAL OF LAW & BUSINESS

VOLUME 14 SUMMER 2018 NUMBER 3

THE LAW AND ECONOMICS OF CYBER RISK POOLING

MICHAEL FAURE AND BERNOLD NIEUWESTEEG*

In this paper, we study the law and economics of cyber risk pooling arrangements: risk sharing without an insurer. We start our discussion with the current theoretical foundations for risk shifting in cyber security. We subsequently discuss cyber risk pooling in relation to individual risk management and cyber insurance. This leads to the formulation of conditions for effective risk pooling in cyber security. We show that pooling, under some circumstances, may be more effective than cyber insurance. The main question for future research is whether risk pools in cyber security are capable of compartmentalization of risks and whether transaction costs of monitoring can be kept sufficiently low.

* Michael Faure is Professor of Comparative Private Law and Economics at Erasmus University Rotterdam, Professor of Comparative and International Environmental Law at Maastricht University, Academic Director of the Maastricht European Institute for Transnational Legal Research, and Academic Director of Ius Commune Research School. Bernold Nieuwesteeg is Director at Centre for the Law & Economics of Cyber Security at Rotterdam Institute of Law and Economics; Ph.D., Law and Economics, Erasmus University Rotterdam. The authors are grateful to Dr. Marco Fabbri and to participants in the seminar on the Future of Law and Economics (Maastricht, the Netherlands, March 2017) for useful comments on an earlier version of this paper. In addition, they thank Bob de Waard en Teun Steenbergen for their research assistance.

Introduction

In the early days of mankind, risk sharing was a rudimentary form of insurance. If someone's vessel was destroyed, neighbors committed to help rebuild it, while at the same time, the owner of the vessel committed to rebuild the neigh-

bor's vessel in case of destruction.[1] This paper takes us back to these forms of risk sharing by examining the concept of cyber risk sharing, also called "pooling." Cyber risk pooling is risk sharing without the interference of an insurer. The concept has received limited attention in the cyber security literature. We aim to contribute to the literature by examining the theoretical potential of cyber risk pooling and by distinguishing the conditions for pooling in order to work in cyber security.

We start the discussion in Part I with the theoretical foundations for risk shifting in cyber security. We subsequently discuss its implications for two traditional risk allocation structures: individual risk management and cyber insurance. When risk allocation changes, incentives for using or obtaining information in order to make socially efficient cyber security investment decisions change.[2] We show that neither individual risk management nor cyber insurance offer perfect incentives for managing capricious risks in cyber security. The last part of this section will introduce cyber risk pooling as a third risk allocation structure. In Part II, we analyze the strengths and weaknesses of risk pooling relative to individual risk management and cyber insurance. Part III addresses earlier experiences with risk sharing, and in Part IV, we summarize conditions for effective risk sharing in cyber security. In Part V, we concretize specific design parameters of a pooling arrangement. We show which design choices should be made in order to fulfill the conditions of an effective risk sharing agreement. We also distinguish the main trade-offs in such a design.

I.
Risk Allocation in Cyber Security

With respect to cyber security, the actor exposed to the risk has incentives to manage it towards its own private opti-

1. Miran Jus, Credit Insurance 7 (2013). Risk sharing was already applied between various operators in the middle ages exposed to similar risk. *See* Göran Skogh, *Risk-Sharing and Insurance: Contracts with Different Institutional Implications, in* Internationalisierung des Rechts und seine ökonomische Analyse: Festschrift für Hans-Bernd Schäfer zum 65. Geburtstag 275, 297–305 (Thomas Eger et al. eds., 2008).

2. Ross Anderson & Tyler Moore, *Information Security Economics – and Beyond*, Presented at the ninth International Conference on Deontic Logic in Computer Science (2008).

mum because he will bear the costs of cyber insecurity.[3] Because exposure to cyber security risk changes in the three risk allocation structures, the structure of risk allocation determines the incentive organizations have in making socially desirable investment decisions.[4] Accordingly, the first aim of this paper is to identify the effects of the three types of risk allocation structures on the incentives of stakeholders involved in reducing the risks related to cyber security. Traditionally, two types of risk allocation structures are taken into consideration by scholars in cyber security, namely, individual management by the individual firm[5] and the (partial) transfer of risk to an insurer in the form of cyber insurance.[6] In this part, we will address these two alternatives in light of their ability to shift risk in an effective manner in cyber security, and stress the need for exploring a third way of managing cyber risks, namely by sharing them amongst firms without the interference of an insurer.

A. *Risk Shifting*

Before addressing these three alternatives for risk shifting, it should be addressed why a demand for risk shifting is created in the first place and why risk shifting may be socially beneficial. In the literature, two foundations for risk shifting are distinguished. The first—the most traditional economic approach—is to consider risk shifting as a remedy for risk aversion.[7] Individuals (and institutions) may have an aversion to risks with a low probability of occurrence but a high degree of potential damage.[8] Given wealth restraints and the limited marginal utility of increasing wealth, individuals suffer disutil-

---

3. Xia Zhao, Ling Xue & Andrew B. Whinston, *Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements*, 30 J. MGMT. INFO. SYS. 123, 126–27 (2013).

4. *Id.*

5. Brent Rowe & Michael Gallaher, *Private Sector Cyber Security Investment Strategies: An Empirical Analysis*, Presented at the fifth Workshop on the Economics of Information Security (WEIS) 2006.

6. Christian Biener, Martin Eling & Jan Hendrik Wirfs, *Insurability of Cyber Risk: An Empirical Analysis,* 40 GENEVA PAPERS ON RISK & INSURANCE 131, 134–35 (2015).

7. *See* STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 258–59 (1st ed. 2004).

8. Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision Under Risk,* 47 ECONOMETRICA 263, 281 (1979).

ity from the risk of being exposed to the possibility of losing a large amount of wealth. Since risk aversion creates disutility for individuals and organizations, social welfare increases if risk is removed from individuals with risk aversion.[9] However, the degree of risk aversion depends not just on the type and the size of the risk, but more particularly on the wealth of the individual concerned.[10] For example, an individual who only possesses €50,000 may be highly averse to a 1% risk of losing €100,000. However, if the same individual possesses several million euro, there would be no risk aversion, and hence no demand to hedge particular risks. This starting point is quite important as it explains that the demand for risk shifting by firms exposed to cyber security will depend upon the type of risk (low probability, high damage, or rather, the reverse) and on the individual wealth situation of the firm concerned.

Therefore, the demand for risk shifting will be high in a situation where the risk to which the firm is exposed is relatively high (in the sense that a high level of damage can occur when the risk materializes) and when the individual wealth of the firm is limited. The latter may more particularly be the case when the potential damage would be greater than the wealth of the firm if the risk materializes. This simple economic logic is also related to the fact that risk shifting is not a costless exercise.[11] Therefore, a willingness to pay for risk shifting will only occur in cases of risk aversion: where the risk is relatively high (i.e., high damage will ensue if the risk materializes) and where firms lack the resources to sustain the risk. This also shows that the attitude to risk and the related demand for risk shifting is not binary (in the sense of all or nothing), but has a gradual nature. The latter may more particularly be important since some techniques of dealing with risk (like individual risk management) have lower costs than others (insurance, for example).

It should, however, be stressed that other justifications for corporate insurance other than risk aversion have also been identified in the literature. Mayers and Smith indicated that the corporate form provides an effective hedge since it allows

9. SHAVELL, *supra* note 7, at 259.

10. Luigi Guiso & Monica Paiella, *Risk Aversion, Wealth, and Background Risk,* 6 J. EUR. ECON. ASS'N 1109, 1122 (2008).

11. Biener, Eling & Wirfs, *supra* note 6, at 144–45.

shareholders to eliminate risk through investment in a diversified portfolio.[12] Since risk reduction is not considered as the most obvious basis for a specific demand for insurance by corporations, Mayers and Smith identify a few other reasons for corporations to demand insurance.[13] One possibility is that corporate insurance contracts allow an allocation of risk to the claimholders of the firm who have a comparative advantage in risk-bearing;[14] insurance may also lower the expected transaction costs of bankruptcy and provide real service efficiencies in claims administration.[15] Also other authors have advanced reasons for risk-shifting (more particularly via insurance), other than risk-aversion.

For example, it has been argued that insurance could reduce information and transaction costs. Operators often wish to benefit from services offered by insurance companies that can reduce transaction costs. Insurers offer the service of administrating claims at much lower cost than corporations would face if claims were to be administered in-house.[16] This is related to the specialization of insurers in claims handling, but also to economies of scale.[17] The advantage for traders is that the contractual conditions in the insurance policy (aiming at the reduction of moral hazard) in fact replace the need for traders to contract in detail, for example, concerning the allocation of risk.[18] This explains why there is a demand for risk shifting by actors who suffer *no* risk aversion as well.[19]

The actors that seek risk shifting in the case of cyber security are mostly commercial operators and not individuals.[20]

---

12. David Mayers & Clifford W. Smith Jr., *On the Corporate Demand for Insurance,* 55 J. BUS. 281, 282 (1982).

13. *Id.*

14. *Id.* at 283–84.

15. *Id.* at 284–86.

16. Göran Skogh, *The Transactions Cost Theory of Insurance: Contracting Impediments and Costs,* 56 J. RISK & INS. 726, 727 (1989).

17. *See* J. David Cummins, *Economies of Scale in Independent Insurance Agencies,* 44 J. RISK & INS. 539 (1977).

18. *See id.*

19. Michael Faure & Donatella Porrini, *Göran Skogh on Risk Sharing and Environmental Policy,* 42 GENEVA PAPERS ON RISK & INS. 177, 180 (2017).

20. *See, e.g.*, Julie Zhu, *Greater China Cyber Insurance Demand Set to Soar After WannaCry Attack: AIG,* BUS. INSIDER (Aug. 9, 2017), http://www.businessinsider.com/r-greater-china-cyber-insurance-demand-set-to-soar-after-wannacry-attack-aig-2017-8?international=true&r=US&IR=T.

As opposed to individuals, corporate actors are often assumed to be relatively risk neutral, especially when they are well-capitalized.[21] However, as will be shown below, there may be a demand for shifting cyber risks—even for corporate actors—precisely due to the specific characteristics of cyber security risks.

B. *Problems in Shifting Cyber Risks*

Assuming that organizations have a demand for shifting cyber risks, the question arises as to whether the particular features of cyber risks are conducive to such risk shifting. Externalities and informational problems, two classic examples of market failures, may arise.[22]

First, externalities cause the costs or benefits of an investment decision to be imposed upon a third party, and thus the party investing does not take into account the full cost or benefit of its decision.[23] For instance, when an organization's computer systems are infected by malicious software that secretly makes them part of a botnet, its systems will be used to execute large-scale attacks against other systems.[24] However, it is in the interest of the person behind the botnet operation to let the initial infection go unnoticed so that the owner of the system will not be prompted to remove the malicious code. The botnet system thus does not even rise to the level of nuisance for the owner of the infected computer. Hence, the benefits of removal of this software belong only to society, which will experience, ceteris paribus, fewer botnet attacks, while the private owner of the initially infected system incurs the costs of detection and removal of the malicious code but few benefits. This poses a problem for society, because there is no incentive for the private owner to remove the malicious code or even

---

21. *See, e.g.*, Eugene F. Fama, *Agency Problems and the Theory of the Firm,* 88 J. POL. ECON. 288 (1980); Mark E. Parry & Arthur E. Parry, *The Purchase of Insurance by a Risk-Neutral Firm for a Risk-Averse Agent,* 58 J. RISK & INS. 30 (1991); Agnar Sandmo, *On the Theory of the Competitive Firm Under Price Uncertainty,* 61 AM. ECON. REV. 65 (1971).

22. *See, e.g.*, George Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism,* 84 Q.J. ECON. 488 (1970); Francis Bator, *The Anatomy of Market Failure,* 72 Q.J. ECON. 351, 356–63 (1958).

23. Carl J. Dahlman, *The Problem of Externality*, 22 J.L. ECON. 141 (1979).

24. Michel van Eeten et al., *The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data* 3 (OECD Sci. Tech. & Industry Working Paper No. 2010/5, 2010).

install programs or otherwise make an effort to detect the infection in the first place.[25] On the other hand, there are also situations wherein the costs of security investment are borne by society, while the benefits are experienced primarily by the private organization. In economic terms: the private investments in risk reduction have an effect on society. But because the private actor cannot internalize these, those risk-reducing actions may not ultimately be taken.

Second, there are informational problems in the cyber market, such as the lack of reliable data about cyber risks and the lack of information about the return on investment for investments in cyber security.[26] The lack of reliable data is a result of the fact that both the type and impact of cyber threats change continuously and it is hard or impossible to forecast future impact based on past data. For example, in recent years, cyber security experts observed a giant spike in *ransomware*.[27] *Ransomware* is a malicious piece of software that takes a computer "hostage," in the sense that the owner cannot access the computer before a certain kind of ransom is paid, usually in the form of a digital currency such as Bitcoin.[28] Thus, long-term data about the frequency of occurrence and average damage is unavailable. Consequently, parties have difficulty in determining proper security measures. This stands in stark contrast to *internet banking fraud*, which declined sharply in the Netherlands after banks undertook effective security measures and is no longer an issue.[29]

---

25. Michel van Eeten & Johannes Bauer, *Economics of Malware: Security Decisions, Incentives and Externalities* 58 (OECD Sci. Tech. & Industry Working Paper No. 2008/1, 2008).

26. *See* SHAVELL, *supra* note 7; MARTIN ELING & WERNER SCHNELL, GENEVA ASS'N, TEN QUESTIONS ON CYBER RISK AND CYBER RISK INSURANCE (Fabian Sommerrock ed., 2016).

27. *See, e.g.*, Alex Hern, *Ransomware Threat on the Rise as 'Almost 40% of Businesses Attacked,'* THE GUARDIAN (Aug. 3, 2016, 8:00 AM), https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked.

28. Alexandre Gazet, *Comparative Analysis of Various Ransomware Virii*, 6 J. COMPUTER VIROLOGY 77 (2010).

29. Total damage of Internet banking fraud in the Netherlands declined sharply from, €4.7 million in 2014 and €3.7 million in 2015 to €148,000 in the first half of 2016. This contrasts with the figures that were measured when Internet Banking Fraud was at the height of its impact in the first half of 2012, when there was €24.7 million damage. *See Hoe Hoog is De Schade Door Fraude Met Internetbankieren?*, NEDERLANDSE VERENIGING VAN BANKEN, https://

Botnets, *ransomware* and *internet banking fraud* are just three examples of cyber risks that are characterized by externalities and informational problems. As we will show, these features of cyber risk compromise the possibility of risk shifting, especially as when it comes to the traditional instrument of insurance.

C. *Cyber Insurance*

Insurance is a technique which provides cover against risk through the (partial) transfer of risks to a third party in return for a premium. However, the premium paid to an insurer will often be substantially higher than the objective value of the risk (the probability multiplied by the damage).[30] One reason for this phenomenon is that insurers may add a risk premium to account for uncertainty or insurer ambiguity.[31] An alternative reason is that insurers may engage in what is referred to as "loading," in which they charge a premium to help cover the high transaction costs required to operate insurance companies.[32] This too explains the gradual nature of the demand curve for insurance: where risk aversion is high, the firm may still have a demand for insurance (even though the premium is higher than the objective value of the risk). If the risks are not assessed extremely highly, the firm may not have a demand for insurance, or may only have a demand to cover higher levels of risk.

In addition to providing a remedy for risk aversion, insurance may also be advantageous for providing the insurer with increased knowledge of efficient investments in cyber security, which it can then transfer to the insured for their mutual benefit. Insurers can benefit from economies of scale in acquiring information on cyber risks.[33] Insurers are able to do this when they have large time window available or are able to aggregate

---

www.nvb.nl/veelgestelde-vragen/veiligheid-fraude/1816/hoe-hoog-is-de-schade-door-fraude-met-Internetbankieren.html (last visited Aug. 5, 2018); *Fraude met internetbankieren 'spectaculair gedaald'*, FINANCIEEL DAGBLAD (Sept. 15, 2016), https://fd.nl/economie-politiek/1167515/fraude-met-internetbanken-spectaculair-gedaald.

30. Robin Hogarth & Howard Kunreuther, *Ambiguity and Insurance Decisions*, 75 AM. ECON. REV. 386, 386–89 (1985).

31. *Id.* at 388.

32. *See, e.g.*, Eric Briys, *On the Theory of Rational Insurance Purchasing in a Continuous-Time Model*, 47 GENEVA PAPERS ON RISK & INS. 165, 171–74 (1988).

33. Biener, Eling & Wirfs, *supra* note 6, at 141.

claim data. By linking premiums to the care level of the insured, insurers incentivize increased care levels of information technology security.[34]

A general problem which often emerges in insuring against relatively new risks is that insurance companies may lack sufficient information to correctly calculate so-called "actuarially fair premiums," which is, as previously mentioned, a particular problem for cyber risks.[35] For example, they may suffer from insurer ambiguity and as a result charge a relatively high risk premium.[36] If the potentially insured firm perceives this risk premium as excessive, supply and demand will not meet. That is the situation where a risk is considered uninsurable. This danger is more likely to occur with newly emerging risks. With new risks, insurers often lack information and will therefore prudently charge (relatively high) risk premiums which may be considered excessive by the individual firm. As a result, the market for insurance for newly emerging risks is often difficult.[37] It is precisely for that reason (i.e., insurers lacking information concerning new risks) that risk sharing by operators may be relatively attractive.[38] Sometimes operators themselves may have better information on the relative nature of the risk than insurers.

Thus, cyber insurance could in theory enable risk shifting, provided there is sufficient information to calculate risks. However, empirical observations show that the market has not yet fully developed, precisely because of the lack of past data, the high premiums that ensue, hard to unravel policies and insufficient awareness among the public. The present cyber insurance market also seems to struggle with a particular feature of cyber security risks which endangers insurability: correlated risks and cascade effects caused by the interconnectedness of IT-systems.[39]

---

34. *Id.* at 145.

35. *Id.* at 144.

36. Howerd Kunreuther, Robin Hogarth & Jacqueline Meszaros, *Insurer Ambiguity and Market Failure,* 7 J. RISK & UNCERTAINTY 71, 79–83 (1993).

37. MICHAEL FAURE & TON HARTLIEF, INSURANCE AND EXPANDING SYSTEMIC RISKS 85–87 (1st ed. 2003).

38. Göran Skogh & Hong Wu, *The Diversification Theorem Restated: Risk-pooling Without Assignment of Probabilities,* 31 J. RISK & UNCERTAINTY 35 (2005).

39. Biener, Eling & Wirfs, *supra* note 6, at 13; Bernold Nieuwesteeg, Louis Visscher & Bob de Waard, *The Law and Economics of Cyber Insurance*

Cyber insurance products have emerged on the market in the early 2000s.[40] Currently, around 10% of European firms have purchased cyber insurance, and this number is probably an order of magnitude lower for small and medium-sized enterprises.[41] The cyber insurance market develops slowly.[42]

D. *Individual Risk Management*

The alternative of individual risk management means that the individual firm will deal with the cyber security risk itself (for example, through security by design and *ex post* risk mitigation), rather than seeking to shift the risk through the purchase of cyber insurance. Individual risk management is therefore not a tool of risk shifting, but rather, as it is sometimes incorrectly termed, a form of "self-insurance."[43] Based on the simple economic logic we just presented, it may be clear that individual risk management will be attractive for dealing with relatively small cyber risks (i.e., only minimal damage will ensue if the risk materializes) or for wealthy firms. To take an example unrelated to cyber security: most large oil and gas producers (often referred to as "the majors") have no demand for insurance to cover risks related to the damage caused by offshore facilities for the reason that they can cover

---

Contracts: A Case Study (LDE Centre for Safety and Security Working Paper); EUR. NETWORK & INFO. SEC. AGENCY, INCENTIVES AND BARRIERS OF THE CYBER INSURANCE MARKET IN EUROPE (2012).

40. Perry Luzwick, *If Most of Your Revenue is from E-Commerce, then Cyber-Insurance Makes Sense,* 3 COMPUTER FRAUD & SECURITY 16, 16–17 (2001); Jay Kesan, Rupterto Majuca & William Yurcik, *The Economic Case for Cyberinsurance*, (Univ. of Ill. L. & Econ. Working Papers Series, Paper No. LE04-004, 2004).

41. *2013 Cyber Risk Survey*, MARSH (June 2013), https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20Survey%2006-2013.pdf. Willis estimates that 6% of the US firms purchased cyber insurance, whereas the Harvard Business Review reports that 19% have done so. WILLIS TOWERS WATSON, WILLIS FORTUNE 1000 CYBER REPORT 4 (2013); *Meeting the Cyber Risk Challenge*, HARV. BUS. REV. (Dec. 12, 2012), https://hbr.org/2012/12/meeting-the-cyber-risk-challen.html.

42. *See, e.g.*, Scott Shackelford, *Should Your Firm Invest in Cyber Risk Insurance?*, 55 BUS. HORIZONS 349, 353–55 (2012); Biener, Eling & Wirfs, *supra* note 6.

43. Self-insurance is not insurance as there is no risk spreading, but usually it just concerns a reservation for future losses. *See* Michael Faure, *Alternative Compensation Mechanisms as Remedy for Uninsurability of Liability*, 29 GENEVA PAPERS ON RISK & INS. 455, 457–58 (2004).

the risk themselves.[44] As a result, British Petroleum (BP) did not have sufficient insurance coverage when the mobile offshore oil rig Deepwater Horizon exploded on April 20, 2010, causing massive damage.[45] Target Corp., which experienced a major data breach in 2013, only had cyber insurance coverage for 36% of the damage.[46] For smaller firms, the potential impact and liability of cyber risks could go well beyond their own solvency.[47]

However, individual risk management also has its limits. In the case of individual risk management, the disutility caused by risk aversion is not remedied. Moreover, the private party has no incentives for the sharing of knowledge among organizations. In the case of individual investment in prevention, the externality problem persists in the sense that there may be underinvestment or overinvestment on the part of the private party relative to the social optimum. In a situation with correlated risks, the firms' security depends on the behavior of others and vice versa. Hence, the incentives for security investments may even be perverse, as third-party behavior possibly negates or increases the payoffs the firm receives from its own investment in protective measures.[48]

E. *A Third Way?*

Neither individual risk management nor cyber insurance offer perfect incentives for managing the capricious nature of cyber risks. A third possible risk allocation structure is cyber risk pooling. Cyber risk pooling is in essence risk sharing between operators without the interference of a third party such

---

44. Michael Faure, Liu Jing & Wang Hui, *A Multilayered Approach to Cover Damage Caused by Offshore Facilities,* 33 VA. ENVTL. L.J. 356, 385 (2015).

45. Michael Cessna, *Insurance Implications of the Deepwater Horizon Disaster,* INS. L. BLOG (May 17, 2010), https://www.lexisnexis.com/legalnewsroom/insurance/b/insurance-law-blog/archive/2010/05/17/insurance-implications-of-the-deepwater-horizon-disaster-by-michael-cessna-of-counsel-lathrop-amp-gage-llp.aspx.

46. *See Target's Cyber Liability Insurance Covered 36% of Its Data Breach Costs. How Much Does Yours Cover?*, INSUREON BLOG (Mar. 24, 2015, 8:25 AM), http://www.insureon.com/blog/post/2015/03/24/how-much-does-your-cyber-liability-insurance-cover.aspx.

47. MICHAEL FAURE & TON HARTLIEF, INSURANCE AND EXPANDING SYSTEMIC RISKS (2003).

48. *See* Howard Kunreuther & Geoffrey Heal, *Interdependent Security,* 26 J. RISK & UNCERTAINTY 231 (2003).

as an insurer.[49] Hans Buhlmann defines risk pooling as follows:

> [A]ny formal mutual agreement among the *n* companies that, operating as an entity, (1) accepts the responsibility for paying for an input . . . (2) charges [companies] an output . . . for accepting the input, according to the agreed-upon rule for sharing risks; (3) operates on a zero-balance conservation principle . . . ."[50]

Provided that certain conditions are met, we argue that cyber risk pooling can potentially move organizations to desirable (hybrid) forms of risk allocation. Cyber risk pooling, as we will argue, can potentially provide *ex post* compensation to risk averse operators to cover damage caused by cyber risks, and at the same time, can contribute to the *ex ante* prevention of cyber risks, thus increasing cyber security within society. In this sense, cyber risk pooling can generate positive externalities for society at large.

II.
Strengths and Weaknesses of Cyber Risk Pooling

In this part, we will discuss pooling relative to individual risk management and cyber insurance. Theoretical studies mention various circumstances in which (cyber) risk pooling might be beneficial for participants and for society relative to individual investment decisions regarding the management of (cyber) security risk.[51] Karl Borch was the first to analyze optimal risk sharing between two parties.[52] Kenneth Arrow discussed various problems related to insurance, such as the inherent problem of moral hazard.[53] Yet it was the Swedish economist Göran Skogh who demonstrated in a seminal 1999 article in the *Journal of Institutional and Theoretical Economics*

49. Cyber risk pooling is also called a form of mutual insurance, or risk sharing, or the formation of risk clubs.

50. Hans Buhlmann & William Jewell, *Optimal Risk Exchanges,* 10 Astin Bull. 243, 245 (1979).

51. *Id.* Buhlmann and Jewell explore general forms of exchange that result in simultaneous improvement of risk for all parties. *Id.*

52. Karl Borch, *Equilibrium in a Reinsurance Market,* 30 Econometrica 424 (1962).

53. Kenneth Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 Am. Econ. Rev. 941 (1963).

that mutual and collective risk sharing between different agents can be beneficial when the probability distribution of losses is uncertain or impossible to estimate.[54] Skogh showed that, as opposed to insurance, mutually beneficial risk sharing is also possible without assignment of probabilities.[55] This is so because in the insurance context, assignment of probabilities is always necessary in order to calculate a premium.[56] In a risk sharing agreement, partners can also share losses *ex post*, as risk sharing is possible so long as the partners in the pool are faced with the same risk.[57] This explains why an insurance market can only reach maturity once considerable actuarial information is available.[58] Thus the concept of risk pooling is not new, but to the authors' knowledge, no practical application of risk sharing in cyber pooling has yet been applied.

A. *Pooling Relative to Insurance*

In this section, we describe the advantages of pooling relative to insurance. In the next section, we compare pooling with individual risk management. The main difference between insurance and risk sharing via pooling is that insurance always requires an assignment of probabilities in order to calculate a premium.[59] Pooling, on the contrary, is more flexible in that it permits even an unpredictable distribution of risks.[60] Operators exposed to a similar risk can share that risk even when the specific probabilities are unknown, while in the insurance context, an unknown distribution of risks prevents in-

54. *See* Göran Skogh, *Risk-sharing Institutions for Unpredictable losses*, 155 J. INST. & THEORETICAL ECON. 505 (1999).

55. *Id.* at 509–10.

56. *Id.* at 506–09.

57. *Id.* at 510.

58. Skogh & Wu, *supra* note 38, at 35.

59. Skogh, *supra* note 54, at 505.

60. John Marshall, *Insurance Theory: Reserves versus Mutuality*, 12 ECON. INQ. 476 (1974). Marshall identified two principles under which insurance might function: the reserve, or transfer, principle and the mutualization principle. Under the reserve principle, risk is transferred to external risk bearers to hold in a reserve from which to discharge claims. With mutualization, policyholders jointly hold the residual claims on the pool. Total losses are shared among policyholders by some combination of prepaid premium and retroactive dividend. The reserve principle is efficient when, by the law of large numbers, the average loss is predictable with virtual certainty while the mutualization principle can be used in more general circumstances. *Id.*

dependent insurers from using the law of large numbers, which assumes that the actual payout on claims will ultimately converge with the average, or expected, payout.[61] Skogh and Hong Wu use the example of ship owners sharing losses to illustrate how risk sharing materializes.[62] Their example involves the sharing of a potential loss of ships and their respective cargo in a situation where no insurance is available. The two ship-owners have a similar ship, cargo, crew and route, and thus the same (unknown) probability of a loss. They would expect to benefit by sharing the loss of a ship. The two ship-owners also realize that the pooling would be more efficient if they could increase the number of partners in the risk sharing group. But the offer to join the pool must be restricted to ship-owners with the same cargo and destination, which could further prove a ship and crew of comparable quality. Limitations on the pooling arrangement exist in the varying value of ship and cargo, as well as varying destinations. But these shortcomings can be solved using a unit of measure called a "share," which permits partners to join the pool with different shares. In this way, the risks at sea can be diversified. Since the pool members have a common interest in the prevention of accidents, they are incentivized to introduce safety regulations according to the information available. As time goes by, they also obtain further information on "high" and "low" risks. The tendency of low risks to leave the pool is mitigated by adjustments in the partners' respective shares, and the benefit of a large pool is thereby maintained.

For Skogh and Wu, the tale paints a plausible picture of the development of pooling and the evolution of insurance, even if experience and historical information may further simplify pricing and thus simplify the trade of risks in the market. Several additional points can be made about risk pooling arrangements. The first is that all participants may beneficially share hazards that are unpredictable or unforeseeable, as long as the presumption of equality is mutually accepted. The question remains whether such a presumption of equality can be established in the case of cyber security risks.

---

61. Neil Doherty & Georges Dionne, *Insurance with Undiversifiable Risk: Contract Structure and Organizational Form of Insurance Firms,* 6 J. RISK & UNCERTAINTY 187, 188 (1993).

62. Skogh & Wu, *supra* note 38.

Second, the pool has the flexibility to develop and issue specialized policies to its members. Risk pools have the flexibility to provide specific coverage or additional coverage beyond the scope of insurance companies.[63] Since risk pool participants are the owners of a risk pool, the usual conflict of interest between insurers and policyholders does not play a role in risk pooling agreements.

Third, total costs can be lower in the case of risk pools. Under an insurance policy, the risk is shifted to the insurer at the price of a premium. The premium is not recoverable by the insured regardless of whether the insured risk materializes or not. Under a risk sharing agreement, a member only contributes if an accident happens; the duty to contribute can either be postponed or the contribution can be carried over to the following year if no accident occurs. A member can also recover his contribution by refraining from creating the risk and leaving the pool. Another cost saving property of risk pooling is that expensive overhead and so called "insurer ambiguity" costs are avoided.[64] The costs of ambiguity can be lower in a risk pooling arrangement since operators exposed to the same risk can be assumed to have better information about the risk than insurers would.[65] In cyber security, this is especially the case when information is shared.[66] Connected to the cost saving argument, a cyber pool might also be beneficial from a liquidity point of view, since money does not "disappear": if nothing happens, it stays in the pockets of the pool's participants.[67]

Fourth, pooling can address the conflicts of interest that arise between the insurer and insured. One of the most prominent conflicts of interest is moral hazard occurring after the insurance contract is closed.[68] For example, the insured might

63. Zhao, Xue & Whinston, *supra* note 3.

64. *Id.*

65. Kunreuther, Hogarth & Meszaros, *supra* note 36, at 72.

66. Florian Skopik, Giuseppe Settanni & Roman Fiedler, *A Problem Shared is a Problem Halved: A Survey on the Dimensions of Collective Cyber Defense Through Security Information Sharing,* 60 COMPUTERS & SECURITY 154 (2016).

67. This depends on the funding structure of the pool. *See infra* Section III.C.

68. Moral hazard is closely linked to adverse selection, which occurs *ex ante*, before signing the contract in situation where complete information is absent. Moreover, it is often hard to distinguish moral hazard from adverse selection in empirical research.

start behaving differently (e.g., take less care) because he himself no longer bears the losses of a damaging event.[69] It is too costly for the insurer to perfectly monitor the behavior of the insured, which can therefore exhibit these undetected actions.[70] In a risk sharing agreement, mutuality is created, whereby the contribution paid by one member depends on the claims made by all other members.[71] It is in the interests of all members' claims to be as low as possible and thus a mutual interest in risk minimization is created.[72] To reduce risks, the members of such a group has incentives both to differentiate risks to align each member's contribution to the risk they pose, and to monitor each other. Mutuality is established when the members are subject to similar safety rules. The members are faced with the same type of risk and often have more expertise and more precise knowledge than a third-party insurer would.[73] This may also be the case in relation to cyber risks, since the participants would have identical IT processes, which would enable them to evaluate the risk each member creates *ex ante*, and in so doing they can better monitor each other's behavior.

Because the likelihood that the members of the pool will have to pay depends on the performance of all members, there will be strong incentives for mutual monitoring. In the event one member attempts to "free-ride" and not take safety efforts seriously this, would create the same moral hazard problem which arises under insurance contracts.[74] Just as monitoring by the insurer is required to cure the moral hazard

69. *See* Steven Shavell, *On Moral Hazard and Insurance,* 93 Q.J. ECON. 541 (1979).

70. Information asymmetry, such as between the insurer and insured, is an important property of cyber security risks. *See* Biener, Eling & Wirfs, *supra* note 6, at 143–44.

71. Paul Bennett, *Mutual Risk: P&I Insurance Clubs and Maritime Safety and Environmental Performance*, 25 MARINE POL'Y 13, 15 (2001). Policyholders are themselves the owners of an insurance pool. *See* Zhao, Xue & Whinston, *supra* note 3, at 126.

72. Bennett, *supra* note 71.

73. Michael Faure & Karine Fiore, *The Coverage of the Nuclear Risk in Europe: Which Alternative?*, 33 GENEVA PAPERS ON RISK & INS. 288, 302 (2008).

74. Wondon Lee & James Ligon, *Moral Hazard in Risk Pooling Arrangements*, 68 J. RISK & INS. 175 (2001) (discussing pool size in relation to moral hazard and insurance).

risk in insurance contracts,[75] in this case the pool members will have strong incentives for mutual monitoring in order to ensure that one risky member does not increase the collective risk.

B. *Pooling Relative to Individual Risk Management*

In the case of individual risk management, there is no risk shifting nor risk sharing whatsoever. In other words, individual risk management does not solve any collective risk aversion since it is only the operator who remains exposed to the risk. To the extent that there is risk aversion as discussed in Section I.A, risk sharing via a pool naturally has advantages. Compared to individual management, risks are naturally better distributed in a risk pool, because they are shared. The actual damage for each policyholder will converge with the average damage based on the law of large numbers.[76] A problem with cyber security risks is the fact that they can correlate, especially when organizations in a pool use similar IT systems vulnerable to similar cyber threats.[77] Unfortunately, this is quite often the case, since IT product vendors are usually large players due to the economics of scale and lock-in effects inherent in the present IT market.[78] Nevertheless, some cyber risks are less likely to correlate, as we shall discuss in Section V.A.

Because the participants in a pool have an equity stake in each other's risk, the positive and negative externalities arising from information security investments can be partially internalized. Insofar as those externalities do not extend beyond the pool members, they will be *fully* internalized.[79]

---

75. Shavell, s*upra* note 69, at 541.

76. *See* Lee & Ligon, *supra* note 74, at 176.

77. For discussion of the trade-off between risk spreading and mutual monitoring, see *infra* Section V.B.

78. *See, e.g.*, HAL VARIAN ET AL., THE ECONOMICS OF INFORMATION TECHNOLOGY: AN INTRODUCTION (1st ed. 2004).

79. Lawrence A. Gordon, Martin P. Loeb & William Lucyshyn, *Sharing Information on Computer Systems Security: An Economic Analysis*, 22 J. ACCT. & PUB. POL'Y 461, 469–70 (2003). This is also the case in insurance, provided that insurers can distinguish these externalities.

C. *Benefits of Pooling Compared to Individual Allocation and Insurance*

In a cyber risk pool, the risk is being shared with other participants, but an operator also takes a part of the risk of other participants in the pool. This creates incentives to cooperate and share knowledge. Based on the literature, we therefore expect that in a cyber risk pool there are strong incentives to share current knowledge and best practices, especially when similar organizations are connected in a risk pool. Some organizations may have more information about efficient risk reduction. A risk pool brings them together, or otherwise brings in an expert to help them (referred to as a managed security service, or "MSS"[80]). In other words, existing knowledge diffuses better amongst the pool.[81] Observe that the first trade-off in risk pooling design emerges here. A homogeneous pool is good for knowledge diffusion and mutual monitoring, while a heterogeneous pool is better from a risk spreading perspective. We will further discuss this trade-off in Section V.B.

Cooperation and knowledge-sharing may eventually even result in more joint (as well as more cost efficient) investment in (external) risk reduction. Joint investments may ultimately produce a set of standards which would make basic cyber security more standardized.

D. *Drawbacks of Pooling*

There are several important drawbacks to the pooling structure. First, an important precondition for mutual risk sharing to work in its most simple form is that the parties in the pool must accept and trust that they all statistically face a similar risk.[82] Parties need to have a similar or at least comparable cyber security risk *ex ante* and need to carry out similar security efforts *ex post*. When this is not the case, the organizations that invest more will eventually drop out of the pool because for them the costs will exceed the benefits. In that sense, there is a danger that a risk pool may be unstable, because there will always be participants in a risk pool with a (slightly)

---

80. Zhao, Xue & Whinston, *supra* note 3, at 126.

81. Gordon, Loeb & Lucyshyn, *supra* note 79; Anderson & Moore, *supra* note 2.

82. Göran Skogh, *Development Risks, Strict Liability, and the Insurability of Industrial Hazards*, 23 GENEVA PAPERS ON RISK & INS. 247, 254 (1998).

better security position (*ex ante* or *ex post*) who will drop out, which may in turn weaken the pool. There is always the problem that pooling may be more attractive for participants that carry high risks. If these risks cannot be adequately identified, adverse selection will prevent pooling from emerging.[83] However, even if risks are *not* homogeneous, this is not necessarily a problem as long as it is possible to differentiate and compartmentalize the risk (for example, by requiring the participant who constitutes a larger risk to pay a larger contribution to the pool).[84]

Second, this danger of free-riding will be worsened when mutual monitoring is impractical or impossible, in which case moral hazard may endanger the pool. As Steven Shavell pointed out: "[w]hen monitoring is impractical, the optimal market response to moral hazard is generally partial insurance coverage."[85] In cyber security, mutual monitoring can indeed be difficult from a knowledge point of view, but those who possess the requisite knowledge are fairly equipped to monitor participants in a pool.[86] This incentive for mutual monitoring will in principle be strong, since the pool has the incentive to control all of its members given that the collective risk will increase if one of its members seeks to free-ride. For technical and highly complicated (new) risks, operators may in some cases have better information (compared to insurers) on optimal preventive technologies, which might include differentiation of the contribution to the pool or exclusion of bad risks from the pool's membership. A question will of course arise: to what extent is the pool able to execute an effective mutual monitoring and thus to control moral hazard and adverse selection? If differentiation between different types of risk would not be sufficiently possible, moral hazard cannot adequately be controlled and there is a likelihood that the pool will not

83. Michael Rothschild & Joseph Stiglitz, *Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information*, 90 Q.J. ECON. 629, 634–37 (1976).

84. *Id.*

85. Lee & Ligon, *supra* note 74, at 176.

86. Interview with Rick Hofstede, Cyber Security Analyst, Redsocks (Oct. 21, 2016).

emerge or that firms reduce their own investment and free-ride on others.[87]

Third, the setup of a pool requires an extraordinary effort and has large positive externalities, which are possibly too large for one party to bear. Since it may be difficult for the participant that sets up the pool to recover the costs it incurs in doing so, he must either do it for altruistic reasons or else stand to receive a very large private benefit from the pool's creation.[88] To overcome this problem with setting up pooling arrangements, a broker might be necessary to set up the pool and "guard" the rules of the game. It that sense, the managed security service proposed by Xue Zhao can also be beneficial, because the private security party spreads knowledge and internalizes externalities.[89]

Another limitation of pooling is the fact that the capacity of the pool may be limited, which would entail that the pooling cannot completely eliminate risk. Additional insurance beyond the cap that is set by the pool might therefore be necessary.

In summation, there are three potential drawbacks of pooling: the pool needs to be able to control the problems of 1) adverse selection, and 2) moral hazard, and 3) there need to be sufficient incentives for the originator to create the pool. Those drawbacks are at the same time also conditions for effective risk sharing. If these drawbacks can be properly addressed, cyber risk pooling may become possible.

III.
Experiences in Other Sectors

Pooling certainly has potential drawbacks, or, formulated differently, there are specific preconditions that must be met in order for pooling to work. Nevertheless, experiences in other sectors show that risk pooling can generate the benefits

87. *See* Bengt Holmstrom, *Moral Hazard in Teams,* 13 Bell J. Econ. 324 (1982).

88. Of course, one of the participants could also initiate the pool and let other participants pay for the pool. However, setting up cyber risk pools is probably not the business of such a private initiator, which makes it extra costly (because there is no experience) to start such a business. Precisely for that reason it is often large brokers that take the initiative to organize a risk sharing agreement.

89. Zhao, Xue & Whinston, *supra* note 3.

described in the literature. In addition to briefly describing the functioning of two existing pools (more particularly the functioning of the so-called "Broodfonds" in the Netherlands and the "P&I Clubs" that cover maritime risks), we will also discuss two other initiatives where the creation of a risk sharing agreement proved more problematic. Examining the reasons why there were difficulties in the creation of the second set of pools contributes to an empirical perspective on the formulation of preconditions for successful cyber pooling.

A. *Broodfondsen*

A Broodfonds (literally, "bread-fund") is a risk pool in which self-employed people share their risks of becoming incapacitated and prevented from working.[90] The main reason why the Broodfondsen emerged in 2006 was because disability insurance for self-employed individuals was expensive. In early 2016, there were 182 Broodfondsen, which even backed *each other* financially, in a form of re-insurance.[91] In an interview with the founder of the Broodfonds, it turned out that mutual monitoring works well, as the self-employed "regularly meet and check upon each other."[92] The checkups also have a social function, since participants also mutually share knowledge and

90. *See, e.g.*, Ties Wiezel, *Ziek en Zelfstandig? Dan is een broodfonds misschien iets voor jou,* NRC (Mar. 23, 2016), https://www.nrc.nl/nieuws/2016/03/22/nrc-q-ziek-en-zelfstandig-dan-is-een-broodfonds-misschien-iets-voor-jou-a1493495; *ZZP Broodfonds: sterk sociaal idee*, STICHTING ZZP NEDERLAND (Nov. 30, 2016), https://www.zzp-nederland.nl/actueel/nieuws/zzp-broodfonds-sterk-sociaal-idee.

91. On Broodfonds' website, the Broodfonds system is described in more detail. "Members of a bread fund group who fall sick receive donations from the other members in their group, the total amounting to a net monthly income. The participants open individual bank accounts dedicated to their 'bread fund'. On these accounts the people who join a *broodfonds* save a fixed amount per month: between €33.75 and €112.50. They also pay a one-time service fee of €250 and a monthly contribution of €10. If members fall sick, they receive net donations depending on their own monthly contribution: between €750 and €2500. Personal donations can be tax-free under Dutch tax law. The monthly savings that accumulate on the bank account of each member are considered as personal savings and when people cancel their participation they collect this sum." BROODFONDS, https://www.broodfonds.nl/hoe_het_werkt (last visited Aug. 5, 2018).

92. Interview with Biba Schoenmaker, founder of Broodfonds (Nov. 2016); *see also Hoe het werkt*, BROODFONDS, http://www.broodfonds.nl/hoe_het_werkt (last visited Mar. 6, 2017).

ideas. All in all, the loss ratios and costs are much lower compared to forms of social insurance for unemployment. It is unclear whether this is created by self-selection or through better monitoring and early checkups.

B. *P&I Clubs*

Another example of mutual risk sharing comes from the maritime context and is provided by the so-called protection and indemnity clubs, or "P&I clubs." A P&I club is a non-profit making mutual insurance association which is established by ship owners and charterers to cover their third-party liabilities related to the use and operation of ships. Today, there are thirteen independent P&I clubs internationally, which collectively account for approximately 90% of the world's oceangoing tonnage.[93]

In the maritime transportation arena, the technical uncertainties regarding the occurrence of oil spills, combined with the legal uncertainties with respect to establishing liability, make it difficult to cover the risk of marine oil pollution using a traditional insurance policy. The P&I clubs appeared as a response to commercial insurers' reluctance to underwrite certain maritime risks.[94] P&I policies cover the liabilities specifically enumerated in the agreement: the club's "rulebook." P&I coverage usually includes unlimited reimbursement for claims arising from: liabilities in respect of persons; liability in respect of cargo, collision with ships, or with fixed and floating objects; salvage; compulsory wreck removal; fines imposed by government agencies; quarantine expenses; towage liabilities; "sue and labor" and legal costs; any other liabilities which the club's directors deem proper to cover; as well as limited reimbursement for oil pollution claims which arise from the members' vessels.[95] The coverage of a P&I policy can be rather

93. *See* IGP&I (Feb. 24, 2018, 6:01 PM), http://www.igpandi.org/about.

94. Norman Ronneberg, *An Introduction to the Protection & Indemnity Clubs and the Marine Insurance They Provide,* 3 U.S.F. MAR. L.J. 1, 25–29 (1990).

95. *Id.* at 7–9. Ronneberg's analysis was based on the Swedish Club's 1990 rulebook. A similar coverage can also be found in the 2010 rulebook of the United Kingdom Mutual Steam Ship Assurance Association (Bermuda) Limited [hereinafter BERMUDA RULEBOOK]. In the rulebooks, the "unlimited" reimbursement does not mean that the Club should pay the full costs which fall into the categories. Instead, the reimbursement is subject to the limitation of liability set by law. While for oil pollution claims, the compensa-

broad: not only does it provide coverage of liability for ecological damage, but the relevant personal injury and property damage as well as other non-environmental losses are also covered. A P&I club provides services beyond those of the typical insurer, operating as an insurance company, law firm and loss adjuster all in one. Besides offering insurance coverage, a P&I club can also provide a worldwide network of correspondents and representatives which can 1) give on-the-spot assistance to the ship owner when required, 2) offer Letters of Undertaking as security when members' vessels are arrested, and 3) assist in claims handling and settlement.[96]

Under the P&I policies, the insured must have suffered actual monetary losses before they can seek reimbursement from the other members. That means a member is only entitled to seek compensation for the amount he has in fact lost due to the occurrence of a covered incident. This is called the "pay to be paid" rule, which is usually incorporated in the club's rulebook. Under a P&I policy, the club is only obligated to assist its contractual counterparts (the club's members) in case of losses. Thus the injured usually cannot bring a direct action against a P&I club and can only obtain the compensation through a claim or litigation against, or settlement with, the injurer.

The P&I Group arranges reinsurance for all the clubs. Presently, under the ship owners' policies, each club retains the first $8 million as their retentions. The amount between $8 million and $60 million is divided among all the clubs. Hydra Insurance Company (the designated insurer of the Group) and the international insurance market also play an important role in providing reinsurance for the upper levels. This brings the upper limit of its reinsurance program to $3.06 billion. Of this amount, the limit for compensation for oil pollution is $1.06 billion.[97]

---

ble sums are determined by Directors of the Club. *See* Rule 5B, BERMUDA RULEBOOK.

96. Ronneberg, *supra* note 94, at 25–29.

97. *See* INT'L GROUP OF P&I ASS'N, 2018 REINSURANCE DIAGRAM, AM. CLUB (Feb. 20, 2018), http://www.american-club.com/files/files/2018_Reinsurance.pdf.

C. *Pooling Offshore Oil Drilling Risks*

There are, however, two examples which show that risk sharing can in some cases be problematic. One is risk sharing in the area of offshore drilling risks. Two risk sharing agreements exist for offshore oil risks: OIL Insurance Ltd. (OIL) and OIL Casualty Insurance Ltd. (OCIL).[98] OIL and OCIL are essentially risk sharing agreements among operators. They provide a maximum coverage of $300 million, but have a high deductible of "not less than $10 million."[99] Notwithstanding the potential advantages of risk pooling arrangements, this type of risk pooling scheme is not very popular in practice. Major operators like BP are relatively critical of these schemes, arguing that they do not sufficiently differentiate the risks involved.[100]

Moreover, detractors argue that the risk pools do not provide full support since, depending upon the contractual arrangements, in some cases the liable operator will be compensated (either by OIL or OCIL) but will have to repay (a part of) the damage over a defined (usually five-year) period.[101] Further, the mutualization between OIL and OCIL make them unattractive to large operators due to the danger of smaller operators free-riding, in which case the majors would become the *de facto* guarantors of the smaller operators.[102]

In this case, the problem is that the damage can potentially be very high, but the probability is very low. Given the relatively low probability of an accident occurring, the difference between an ideal risk and a large risk may be that the ideal risks contribute $30 thousand dollars each and the large risks $60 thousand. That difference is simply too small: the large risk could simply pay a contribution and then free-ride on the ideal risks which have to contribute following an accident. Pools thus provide a safety net of sorts for smaller players with limited balance sheets, and the risk differentiation in-

98. Regis Coccia, *Munich Re Outlines Liability Coverage Innovation for Offshore Oil Risks,* BUS. INS. (Dec. 9, 2010, 12:00 AM), http://www.businessinsurance.com/article/20100912/NEWS/100919977.

99. Faure, Liu & Wang, *supra* note 44, at 389–90.

100. Interview with representatives of BP (Mar. 26, 2013).

101. Interview with representatives of OGP (Feb. 25, 2013).

102. Interview with representatives of Shell International BV, in Rotterdam, Neth. (Mar. 14, 2013).

volved is simply insufficient.[103] In essence, the problem of adverse selection cannot be cured, as major players fear that they are being asked to back up smaller players without sufficient risk differentiation.

D. *Ria de Vigo*

Another failed risk sharing agreement (on a much smaller scale) was attempted on the Ria de Vigo in Northwest Spain.[104] In this risk sharing agreement, several fisheries would share risks for marine pollution, such as oil spills. A study showed that although a risk sharing agreement could be very beneficial for operators in the particular region, many misperceptions and objections inhibited the creation of a risk sharing agreement. Some operators confused risk sharing with commercial, for-profit insurance; others did not understand that a risk sharing agreement would allow the transfer of risk and conceived of it as a clearing house of sorts to transfer money. In the particular case of the Ria de Vigo, the creation of a risk sharing agreement failed largely as a result of insufficient understanding of the benefits and operation of the proposed scheme and apprehensions about free-riders abusing the arrangement.[105] This example clearly shows the importance of good communication about the potential benefits of a risk sharing agreement among the operators to be exposed to the risk in question.

IV.
Conditions for Effective Cyber Risk Sharing

In Part III, we discussed the benefits and drawbacks of pooling in comparison with individual management and cyber insurance. The examples show that risk sharing can be an attractive tool to protect risk-averse actors by generating large amounts of compensation and providing better risk prevention through mutual monitoring. The same benefits can theoretically be obtained in the cyber security market as well. However, both theory and practice show that risk sharing may not

103. *Id.*

104. Schimon Grossmann & Michael Faure, *Conditions for Effective Risk Sharing Against Marine Pollution: The Case of the Ria de Vigo, NW Spain*, 2 Envtl. Liability. 59 (2016).

105. *Id.* at 68.

be able to generate those benefits under all circumstances. Based on both the literature and examples from other sectors, we can distinguish three main preconditions for effective risk sharing, which we will analyze.[106]

A. *Sufficiently Unattractive Alternatives*

The first condition is that the alternatives to pooling, namely individual management or cyber insurance, must be sufficiently unattractive. In the case of P&I clubs we observed pooling in situations where insurers did not want to enter the market while at the same time the harm of an individual incident exceeded the solvency of any individual organization. In the case of the Broodfonds we observed that the insurance alternative was priced insufficiently competitively due to, high information costs (among other things), while simultaneously the risk of incapacitation was too large for any one individual to bear.[107] The fact that the alternatives were sufficiently unattractive is of course related to the theoretical advantages of risk shifting via pooling which we have sketched above in Section II.C. Especially for new risks like in the cyber security context, insurance may suffer from high insurer ambiguity (with resulting risk premiums that are relatively high) and from the impossibility of calculating actuarially fair premiums.[108] Individual risk management may be relatively unattractive as it does not involve risk shifting and therefore neither provides *ex post* compensation, nor diffusion of information that could contribute to *ex ante* prevention. Cyber risk pooling can be relatively attractive compared to those alternatives as it allows pooling even when the statistical probabilities of incidents occurring are unknown (which insurance does not allow for) and since it can provide 1) *ex post* compensation for damage, 2) lower transaction costs, and 3) the sharing of information which could enhance *ex ante* prevention (which individual risk management does not provide).

106. Not surprisingly the conditions for an effective risk-sharing also relate, as we will show, to the conditions for the insurability of particular risks. *See, e.g.*, BARUCH BERLINER, LIMITS OF INSURABILITY OF RISKS (1st ed. 1982).

107. Interview with Biba Schoenmaker, Founder, Broodfonds (Feb. 11, 2016).

108. Biener, Eling & Wirfs, *supra* note 6.

B. *Effective Mutual Monitoring*

As was made clear above in Section II.D, a second condition is that the problems of adverse selection and moral hazard must be controlled.

Cyber risk pooling is obviously easiest if all participants in the pool would statistically be facing a similar risk.[109] In that case, problems of adverse selection would not arise. However, risk sharing of course need not require pure homogeneity. If, for example, two farmers would conclude a risk sharing agreement for the risk of their farmhouses being destroyed, risk sharing is still possible even if one farm is double the value of the other, which might simply entail that the farmer with the more expensive house has a larger share in the pool.[110] So too in the case of cyber risks, the participants in the pool may not all constitute homogeneous risks. Pooling is still possible as long as the relative contribution of each participant in the pool can be appropriately distinguished and be related to his contribution. Also during the duration of the pool's operation, mutual monitoring is necessary to cure the problem of moral hazard.[111] In cyber risk pools, this can be done through the use of network monitoring, where either the participants of a pool or a third party continuously scan the network traffic of each participant. Network monitoring can be complemented by mutual audits at regular intervals of the structure of the IT architecture and the up-to-datedness of software. The incentive for mutual monitoring will in principle be strong, because the pool has the incentive to control all of its members since the collective risk would increase if one of the members attempts to free-ride. The different risks brought into the pool by various participants can be reflected in a differentiation of the contribution to the pool or in an exclusion of bad risks from the pool's membership. A question will of course arise to what extent the pool is indeed able to execute an effective mutual monitoring and thus to control moral hazard and adverse selection. If a differentiation between different types of risk would not be sufficiently possible, moral hazard cannot be adequately controlled and there is a likelihood that the pool will not emerge.

---

109. *See* Skogh, *supra* note 82. *See also* Section V.B.
110. *See* Skogh, *supra* note 1, at 297–305.
111. Skogh, *supra* note 82.

Mutual monitoring needs to take place with only limited transaction costs. These transaction costs will be lower when risks are similar or at least comparable. In principle, since subjective probabilities do not need to be known *ex ante*,[112] risk sharing does not require past loss experience or statistical information (though again, these can lower costs). In a cyber risk pool, a trade-off needs to be made as to the extent each wants to monitor the other. With regard to network monitoring, there are fixed costs and economies of scale in the technical set up of a monitoring system. These costs logically decrease when similar IT systems must be monitored. Moreover, even when companies themselves have little experience and knowledge in cyber security, they can hire IT consultants to undertake the monitoring of the cyber security. Those consultants often do have the required expertise to be able to adequately monitor the level of cyber security of the partners in the pool. However, the automatic detection of anomalies in a monitoring system always leaves a residual which requires a manual analysis at a relatively high variable cost.[113] Lastly, mutual trust can lower these costs because it reduces the need for perfect mutual monitoring.

C. *Practical Possibility of Setting Up a Pool*

A practical condition for effective risk sharing is that there must be a practical premise for creating the pool, which usually requires a party willing to take the initiative in setting up the pool. This requires not only that the potential participants are sufficiently aware of both the cyber security risks to which they are exposed and the benefits of pooling, but even if those conditions are met, there may arise the difficulty that it is simply costly and complicated to start a pool. Not only does it require a sufficient number of participants in order to have adequate risk spreading, but someone needs to take the initiative. This could lead to substantial start-up costs. Pooling therefore either requires one participant with a potentially large interest in starting a pool or a third party (in practice often a broker) who is able to initiate the pool cost effectively. In both cases the upfront costs for setting up the pool can of course be later

112. Skogh, *supra* note 1, at 297–305.

113. Interview with Steffen Morrees, Cyber Security Analyst at Fox IT (May 10, 2017).

recovered from the participants. A degree of trust *ex ante* is likely beneficial for the start-up process. For example, in an environment of trust, participants are more likely to be tolerant regarding the possible existence of slight inequalities in the size of each participant's share in the pool.

V.
The Design of a Cyber Risk Pool

Cyber pooling, as has been shown, has advantages compared to individual cyber risk management and may be able to provide coverage in cases where cyber insurance may not be able to. But risk sharing also has particular drawbacks and therefore conditions that must be met for pooling to emerge. This part discusses the main design parameters for risk pool contract design in cyber security.

A. *The Covered Risks*

A risk pool is an alternative form of risk management. The first design parameter to discuss is thus, naturally, the choice of risks to include in the pooling arrangement. We discuss four perspectives for determining suitable cyber risks for coverage in pooling.

1. *Impact*

A first criterion is the impact of the risk. The impact of the risk is of course directly related to the economic aspect of risk aversion. As indicated above, a demand for risk shifting will emerge principally in the case of relatively large risks, that is, risks whose magnitude goes beyond the individual capacity of operators. Risks that have a small potential impact are easily manageable by individual organizations.[114] A demand for risk sharing via pooling will only emerge for risks that have a higher magnitude. *Personal data breaches* can result in significant costs, which may consist of, for instance, legal sanctions, disclosure and mitigation costs and reputational damage.[115] However, a problem may equally arise with so-called cata-

114. *See* Zhao, Xue & Whinston, *supra* note 3 (arguing that risk sharing, or RPA, which stands for Risk Pooling Arrangement, is ineffective if the risks are sufficiently small).

115. Bernold Nieuwesteeg, The Legal Position of Societal Effects of Security Breach Notification Laws (TU Delft, 2014).

strophic, or high impact, risks. High impact risks, especially those on a level that is not bearable even once distributed across the participants of the pool, are not suitable for pooling either, because the damage of an individual incident exceeds the solvency of the participants in the pool. The exact expected damage of cyber risks is often hard to determine.[116] However, as discussed in Section II.A, pooling arrangements are more flexible when it comes to unknown distributions of risk. A widely-used approach to determining *ex ante* which risks are included in a risk pooling arrangement is to set caps and deductibles that basically set an impact interval within which the pooling arrangement applies.[117] With the right cap and deductible, an *ex ante* determination of the potential impact of risks is no longer necessary. Correlated risks, whereby multiple or even all the participants in a pool experience high impact at the same time, remain an issue. To mitigate the risk of correlated risks, the cap must be sufficiently low, or there must be a form of reinsurance in the case of a strong correlation of risks.

2. *Hybrid Models*

A pool that uses deductibles and caps is often part of a hybrid model where all three risk allocation structures (individual management, pooling, cyber insurance) are used. A cyber risk pool is almost always a part of multilayered approach:

Below the deductible, the participant individually manages its risk. This makes sense, because bearable risks should not be shared or transferred.[118] These are risks (e.g., minor data loss or subsets of larger risks) that are too small to require risk sharing.

Medium-sized risks are suitable for pooling. The question is what exactly, in terms of damage, are medium-sized risks in cyber security? An initial estimation could for example determine the interval of medium size risk to be between €500,000

116. For discussion of the nature of cyber risks, see *supra* Section I.B.

117. A cap is a maximum amount for the payout. A deductible is an amount that must be paid by each participant in the pool before the common pool will pay.

118. For discussion of the theoretical foundations of risk shifting, see *supra* Section I.A.

and €5 million (roughly between $590,000 and $5.9 million). Examples may include severe DDoS attacks or significant loss of personal data. The maximum cap could be heightened through reinsurance, possibly among several risk pools.[119]

For catastrophic cyber risks, risk sharing will not work, as the pool may simply lack the capacity to deal with these losses. Reinsurance can then capture the residual risk up to a certain level. Thus, reinsurance is a possible solution, but in the current cyber insurance environment, both deductibles and caps appear to be relatively low.[120] The insurance would then consist of a so-called excess insurance where the coverage is only taken for damage above a certain level. In the previous example, it would consist of damage above €5 million up to the limit of the insurable amount. Insurers use relatively low caps and low deductibles, while this type of product would require a high cap and (very) high deductibles.

3. *Impact of Care Measures*

It is important to study the effect of care measures on risk reduction. It is desirable to pool risks that are relatively independent from the care measures of the participants in the pool. In such a situation, there will be less free-riding and moral hazard because there is little or no relation between the activity level of the participant and the size of the risk. Hence, it is desirable when cyber risks occur exogenously, that is, cyber-attacks that are relatively independent from the cyber investments of the participants in the pool. For instance, *banking Trojans* seem to occur relatively randomly at US banks.[121]

4. *Systemic Risks*

Another important aspect is the correlation between incidents of cyber risks. One major issue for both insurance and pooling is that cyber risks tend to correlate because they have a systemic character. Correlated risks, unfortunately present in

119. Brokers like Marsh and Willis provide these services, but only for very large companies. The Broodfonds organizes reinsurance with other pools in de Broodfonds.

120. Nieuwesteeg, Visscher & De Waard, *supra* note 39.

121. Samaneh Tajalizadehkhoob et al., *Why Them? Extracting Intelligence about Target Selection from Zeus Financial Malware* (unpublished working paper presented at the thirteenth Annual Workshop on the Economics of Information Security (WEIS)) (2014).

cyber security at least on a theoretical level, hamper efficient risk sharing. Correlation can be an important impediment to an effective sharing of cyber risks.[122] Correlation implies that all companies in the pool are affected, and moreover, that the losses in the pool are significant. Thus a trade-off is presented: on the one hand, comparability of the risks would make mutual monitoring and pooling easier; on the other hand, it could increase the possibility of correlation and therefore the risk exposure of the pool. One option to mitigate the risk of correlation is to focus on those types of risks which have high internal (but low cross-organizational) correlation, such as insider attacks.[123]

B. *Size and Type of Participants in the Pool*

In this section, we show the main trade-offs when choosing between smaller or larger groups (size of pool), when selecting either homogeneous or heterogeneous groups (type of participants), and when choosing the organizational size of the participants.

1. *Group Size*

We assume that the degree of internalization of societal risk increases if group size increases. Large groups are better capable of internalizing externalities because they form a larger part of society. Moreover, in order to create a sufficient degree of risk spreading, there needs to be a reasonably large group. The law of large numbers becomes more accurate as the group size increases. Consequently, larger groups will tend to approach socially optimal behavior better. An increased group size therefore better enables risk sharing.[124] However, with larger groups, information costs also increase. This is caused by the fact that there are higher transaction costs involved in mutual monitoring. Consequently, *ceteris paribus* (all else being equal), larger groups will experience a greater concern of moral hazard and of adverse selection. The impact of

122. So also with respect to the insurability of cyber risks. *See* Biener, Eling & Wirfs, *supra* note 6.

123. Rainer Bohme & Gaurav Kataria, *Models and Measures for Correlation in Cyber-Insurance* (unpublished working paper presented at the fifth Annual Workshop on the Economics of Information Security (WEIS)) (2006).

124. Lee & Ligon, *supra* note 74.

individual free-riding on the personal risk distribution is also lower in larger groups, which decreases incentives to correct other participants. Yet from a practical point of view, it is easier to set up a smaller pool than a larger one. Therefore, a sufficient number of firms (but not too many) should be included, all of which ideally face a similar risk, thereby making possible an effective diversification of risk.[125] In practice, we have observed that effective risk pools have between 10 and 30 members.[126]

2. *Type of Participants*

The type of participants is defined as the degree of homogeneity among the participants, or in other words, the similarity in the size of the organizations, IT processes, customers, etc. Homogeneous organizations have fewer costs in monitoring each other so as to avoid adverse selection and moral hazard. For instance, if operators have the same software systems, then mutual monitoring is straightforward, but also the risk of correlation is higher and consequently risk spreading is lower. Further, homogeneity is a catalyst for knowledge diffusion, especially in cyber security. Consider a *Zero-Day* hack of one of the participants in the pool.[127] A *Zero-Day* threat is an undiscovered vulnerability that can be exploited by an attacker. Once the attack has been successfully executed, attackers will further utilize the *Zero-Day* by executing attacks at similar organizations. Those vulnerable organizations are likely to include the other participants in a homogeneous pool. After a while, either a member of the pool or a third party such as the software vendor will discover the *Zero-Day*. In such a situation effective knowledge-sharing about the origins of the attack and solutions to fix it can greatly reduce overall damage within the pool. Note that here, the speed of the knowledge diffusion is the main advantage. Moreover, setting up a risk pool is easier when organizations do not vary widely in size and type, because a baseline defense effort can be established more easily.

125. Skogh, *supra* note 82, at 254.

126. We observed this amount of members, inter alia, at the Dutch Broodfonds. *See supra* Section III.A. Also P&I groups usually have a size of this magnitude.

127. Interview with Steffen Morrees, Cyber Security Analyst at Fox IT (May 10, 2017).

Recall the difficulties in setting up a risk sharing scheme in the field of offshore oil pollution: since there are large differences between the so-called major oil and gas producers on the one hand, and smaller- and medium-sized enterprises on the other, it is difficult to create a risk sharing agreement in which those largely diverging risk types can jointly participate.[128] As was mentioned above, differences in risk profile between the members of the pool are not necessarily a problem as long as this can be recognized and compartmentalized by the pool members. In such a case, principles of risk differentiation can be applied (by requiring larger shares from the higher risk members). A differentiation of the contribution in that sense constitutes an adequate remedy for moral hazard and also provides incentives for prevention. On the negative side, there is more correlation between cyber risks when there is more homogeneity amongst participants in the pool, as it is likely that similar organizations use similar software systems and are vulnerable to similar kinds of attacks. Hence, there is a trade-off between *heterogeneity* and *homogeneity*. Heterogeneity allows for a better distribution of cyber risk, while homogeneity allows for better mutual monitoring, lower costs and faster knowledge diffusion.

3. *Effects of Participant Size*

As the example of risk sharing in the offshore oil pollution sector shows, the operators' attitudes towards risk (which is strongly related to their financial capacity) will strongly affect the demand for risk shifting and hence the willingness to participate in a pool. This same problem will be relevant in the case of sharing cyber security risks. The demand for risk shifting can be expected to be higher among relatively small and medium-sized operators than among larger operators. Larger operators may be able to cover most risks themselves and thus have less demand for risk sharing. Moreover, larger operators may even fear that small- and medium-sized operators would free-ride given the mere size of the larger operators. This free-riding problem was the reason it was so difficult to create a risk sharing pool for oil pollution in the offshore sector and may to some extent play a similar role in case of cyber security. One way of potentially solving the problem is to create several risk

128. *See supra* Section III.C.

pools with different types of players, each constituting relatively homogeneous groups. The obvious solution would then be to create one group for small- and medium-sized operators and one for larger operators (to the extent that they have a demand for risk shifting at all). Separating those risks into different risk pools may, moreover, improve risk differentiation and thus better stimulate the preventive function of risk sharing.[129] A cyber risk pool that aims to deploy some kind of technical mutual monitoring solution arguably would need to consist of at least medium-sized companies, because otherwise the costs of such a monitoring solution would outweigh the benefits.

C. *Rules of Entry*

One of the key determinants of a successful risk pool is its ability to successfully monitor and select its participants *ex ante* in order to reduce adverse selection. A degree of ex ante cyber security is also important to disentangle the impact of the risk from the care measures of the members of the pool, which, as argued in Section V.A, is preferable in order to reduce free-riding. If all members implement a level of security *ex ante*, attacks that take place can be reasonably believed not to result merely from careless behavior. Consider the example of *ransomware* discussed in Section I.B. *Ransomware* is widely used by cybercriminals. However, an organization could greatly reduce the risk from *ransomware* by implementing certain simple care measures *ex ante*.[130] In the case of a cyber risk pool, it can be difficult or time-consuming to determine the level of cyber security *ex ante*. A third party, such as a security firm, can objectively determine the level of security necessary to be implemented *ex ante* by performing a network assessment and issuing a certification. Often these certifications by private certifiers will be used as proof of compliance with particular security rules. Another option is to assume a given *ex ante* security level and to set this level as a precondition for payout *ex*

129. *See* George Priest, *The Current Insurance Crisis and Modern Tort Law,* 96 YALE L.J. 1521 (1987). Priest strongly stresses the importance of segregating risks into relatively small risk pools with similar risks in order to prevent adverse selection.

130. Interview with Steffen Morrees, Cyber Security Analyst at Fox IT (May 10, 2017).

post. In a cyber risk pool, one could require extensive *logging*, which would allow for tracing back the origins of the cyber attack and determining the organization's level of cyber security at the moment of attack. Moreover, government or private regulation can also assist in determining the required level of cyber security. Further, several design options are possible as to the decision-making regarding the entry of new participants. In the Broodfonds example, the members of the pool must agree unanimously to include a new participant in the pool. In this respect, an important role would be played by the administrator of the fund (usually a broker).

D. *Contribution of Each Participant*

The most standard form of contribution is that every participant has an equal stake. However, this provides an advantage to those participants which are more likely to experience risk and are thus incentivized to free-ride. In more complex situations where the risk of individual participants differs, (a mix of) other metrics can be used as a proxy for determining the proper level of contribution, including bandwidth, turnover and the average number of connected devices or data records. In such a situation, there is a risk that larger players will not want to participate in the pool because of the prospect of free-riding by the smaller players, and this is especially the case when the gap between the two groups is wide. In order to institute optimal incentives for prevention, it may be clear that the contribution should, in principle, be risk-related. "Good" risks should therefore contribute less than bad risks do. This risk differentiation, as reflected in the financial contribution, will provide incentives for prevention. The reverse would be the case in the absence of risk differentiation, in which case a flat fee contribution would be charged. Such a flat fee would invite free-riding as it would not provide any rewards for investing in additional safety measures. Most existing risk sharing agreements (including the P&I clubs) should therefore impose minimum safety rules on the one hand, and differentiate financial contributions according to risk on the other. In order to provide adequate incentives for prevention, the latter approach should also be used for cyber security risks. Minimum *ex ante* safety rules could for instance be determined through the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC)

27002 and the Centre for Internet Security's (CIS) Critical Security Controls.

E. *Timing of the Contribution*

There are various ways to fund a pool. Buhlmann and Jewell distinguish three types of risks pools.[131]

1. *Paying Ex Ante*

By paying a premium *ex ante*, all participants pay a periodic fee. For example, the members of the Broodfonds pay a monthly premium to each Broodfond's bank account. The major advantage of requiring up-front payment is that the willingness of all participants in the pool to contribute to the pool will be higher *ex ante*, when they do not know who will be victimized by the cyber security risk and the decision is being taken "behind the veil of ignorance." It avoids the problem of hindsight bias, which creates a reduced willingness to contribute *ex post* on the part of members who were not ultimately victimized. However, the disadvantage of an *ex ante* payment is that it leads to an immobilization of capital.

2. *Paying Ex Post*

Paying *ex post* means that participants in the pool solely pool the risk, and then pay per claim *ex post*.[132] The advantage of this system is that members retain liquidity and there is no welfare loss caused by "dead" money. However, uncertainty is increased since members cannot be sure that the other members will pay. A possible means of avoiding this uncertainty is through a bank guarantee, as is used in a European system to cover pollution damage for offshore oil and gas installations known as the Offshore Pollution Liability Agreement (OPOL). OPOL guarantees that specific funds will be made available to meet the claims by having its members provide proof of financial wherewithal. OPOL provides de facto mutual risk sharing as far as the insolvency of one of its members is concerned. For that reason the solvency of the members is controlled since

131. Buhlmann & Jewell, *supra* note 50.
132. This is called a claims pool. *See id.*

operators have different ways of demonstrating financial wherewithal.[133]

3. *Hybrid Payment*

In the case of *ex ante* payment, the claims could exceed the accumulated funds. In such a situation, a hybrid framework—a combination of prepaid premium and retroactive dividend—is one solution.[134] In practice, many existing risk sharing agreements use a hybrid model. For example, the P&I clubs discussed above will, in principle, demand an upfront payment from their members. When a "good" year (one with few or no losses) occurs, the club could decide not to require a contribution for the following year. Conversely, during an especially "bad" year (with relatively large incidents of damage) a request for additional funds can be made of the members.[135]

CONCLUSION

In this paper we analyzed the potential for, and conditions precedent to, using risk pooling as a tool to deal with cyber security risk. Risk pooling has often emerged as an alternative to insurance for newly emerging risks. With newly emerging risks, statistical information which would allow an accurate pricing of the risk is often unavailable, and the ensuing insurer ambiguity may lead to high risk premiums as a result of which there may be insufficient demand. The basic idea with risk pooling is that when it comes to particular risks, operators may have better information than insurers on both the risk exposure and on the optimal preventive measures to be taken. When this is the case, a pool can lead to mutual monitoring, which serves to stimulate 1) information exchange, 2) a reduction of transaction costs, and 3) *ex ante* prevention of risks. We posited that if these conditions are present, risk pooling may create protection not only for individual operators who participate in the pool, but also positive externalities for

133. For details see Michael Faure & Hui Wang, *Compensating Victims of a European Deepwater Horizon Accident: OPOL Revisited*, 62 MARINE POL'Y 25 (2015).

134. Marshall, *supra* note 60.

135. *See* Michael Faure, *In the Aftermath of the Disaster: Liability and Compensation Mechanisms as Tools to Reduce Disaster Risks,* 52 STAN. J. INT'L L. 95, 155–57 (2016).

society at large, since the pool can contribute to the general reduction of cyber security risks.

The main advantage of risk pooling is that it can provide coverage even when the specific probabilities of an incident occurring remain hard to predict. Whereas insurance always requires the setting of a premium, pooling is possible without a specific pricing of the risk. It is necessary, however, to identify the relative contribution of the various participants to the pool.

Based on these general starting points we examined the potential of risk pooling in the cyber security context. We argue that if sufficient information can be gathered by operators to enable differentiation of the relative risk exposure for, and contribution of, the various participants, then the traditional problems of adverse selection and moral hazard (which both threaten the emergence of risk pooling) can be remedied. We also noticed that the major advantage of cyber risk pooling primarily lies not in compensation *ex post* (for which insurance is often used), but rather in the information exchange that may be generated through the creation of a pool.

Referring to examples of both viable and failed risk pools, we pointed at the importance of implementing a careful design for the cyber risk pool. To the best of our knowledge, cyber risk pooling has not yet emerged. However, we argue that there may be strong incentives among operators to create such pools, not so much as tools for *ex post* compensation, but as tools for information exchange which can produce *ex ante* reduction of cyber security risks. The emergence of a risk pool, however, requires both a somewhat accurate understanding on the part of operators of the cyber security risk at issue, as well as a degree of similarity (perhaps even homogeneity) among the risks faced, in order to facilitate the risk pooling. It also will most likely require an active entrepreneur like a broker to initiate the pool. Moreover, risk pooling would never be the *only* instrument used to deal with cyber security, both from a prevention standpoint as well as from a compensation perspective. With respect to compensation, a pool would likely include a large deductible, which would mean that operators would still individually manage risks below the deductible, and in doing so, reduce moral hazard. Moreover, pools usually include important limits—very high, catastrophic risks are often hedged to (re)insurers. It is therefore likely that in the future,

cyber risk pooling may come to take an important place in multi-layered compensation mechanisms for dealing with cyber security risk.

The goal of our paper was merely to postulate that risk pooling could play an important role in cyber security and to show the specific conditions and design issues that would have to be taken into account in developing cyber risk pooling. Of course, the specific nature of the cyber security risk, as well as the wide variety of cyber risks, deserve further attention. The results of such research may ultimately warrant the conclusion that various risk pools will be required for specific types of cyber security risks. Both the finding of a means to design such a system in a more detailed manner, as well as the interest of operators in participation in such a pool, are issues that undoubtedly merit further research.